

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-03/msg00341.html>

- *From:* Cisco Systems Product Security Incident Response Team <psirt@xxxxxxxx>
 - *Date:* Wed, 26 Mar 2008 17:00:00 +0100
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

Advisory ID: cisco-sa-20080326-dlsw

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-dlsw.shtml>

Revision 1.0

For Public Release 2008 March 26 1600 UTC (GMT)

Summary

=====

Cisco IOS contains multiple vulnerabilities in the Data-link Switching (DLSw) feature that may result in a reload or memory leaks when processing specially crafted UDP or IP Protocol 91 packets.

Cisco has released free software updates that address these vulnerabilities. Workarounds are available to mitigate the effects of these vulnerabilities.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-dlsw.shtml>

Note: The March 26, 2008 publication includes five Security Advisories. The Advisories all affect Cisco's Internetwork Operating System (IOS). Each Advisory lists the releases that correct the vulnerability described in the Advisory, and the Advisories also detail the releases that correct the vulnerabilities in all five Advisories. Please reference the following software table to find a release which fixes all published Security Advisories as of March 26th, 2008.

* March 26th bundled IOS Advisory Table

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-bundle.shtml>

Individual publication links are listed below:

* Cisco IOS Virtual Private Dial-up Network Denial of Service Vulnerability

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-pptp.shtml>

* Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-dlsw.shtml>

* Cisco IOS User Datagram Protocol Delivery Issue For IPv4/IPv6 Dual-stack Routers

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-IPv4IPv6.shtml>

* Vulnerability in Cisco IOS with OSPF, MPLS VPN, and Supervisor 32, Supervisor 720, or Route Switch Processor 720

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-queue.shtml>

* Cisco IOS Multicast Virtual Private Network (MVPN) Data Leak

<http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml>

Affected Products

=====

Vulnerable Products

+-----

This security advisory applies to all Cisco products that run any version of affected Cisco IOS software configured for DLSw. Systems that contain the DLSw feature, but do not have it enabled, are not affected.

Routers enabled for DLSw contain a line in the configuration defining a local DLSw peer. This configuration can be observed by issuing the command "show running-config". Systems configured for DLSw contain lines similar to the following:

```
"dlsw local-peer"
```

or

```
"dlsw local-peer peer-id <IP address>"
```

Any version of Cisco IOS prior to the versions which are listed in the Software Versions and Fixes section below is vulnerable.

To determine the version of Cisco IOS software running on a Cisco product, log in to the device and issue the show version command to display the system banner. Cisco IOS Software will identify itself as "Internetwork Operating System Software" or simply "IOS". On the next

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

line of output, the image name will be displayed between parentheses, followed by "Version" and the IOS release name. Other Cisco devices will not have the "show version" command or will give different output.

The following example identifies a Cisco product running Cisco IOS Software Release 12.3(6) with an installed image name of C3640-IS-M:

```
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-IS-M), Version 12.3(6), RELEASE SOFTWARE (fc3)
```

The next example shows a product running Cisco IOS Software Release 12.3(11)T3 with an image name of C3845-ADVIPSERVICESK9-M:

```
Cisco IOS Software, 3800 Software (C3845-ADVIPSERVICESK9-M), Version 12.3(11)T3, RELEASE
SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
```

Additional information about Cisco IOS release naming can be found at <http://www.cisco.com/warp/public/620/1.html>.

Products Confirmed Not Vulnerable

+-----

Cisco IOS devices that are not configured for DLSw are not vulnerable.

No other Cisco products are currently known to be affected by these vulnerabilities.

Details

=====

Data-link switching (DLSw) provides a means of transporting IBM Systems Network Architecture (SNA) and network basic input/output system (NetBIOS) traffic over an IP network. Cisco implementation of DLSw also uses UDP port 2067 and IP Protocol 91 for Fast Sequenced Transport (FST).

Multiple vulnerabilities exists in Cisco IOS when processing UDP and IP protocol 91 packets. These vulnerabilities do not affect TCP packet processing. A successful exploitation may result in a reload of the system or a memory leak on the device, leading to a denial of service (DoS) condition.

Cisco IOS devices configured for DLSw with "dlsw local-peer" automatically listen for IP protocol 91 packets. A Cisco IOS device that is configured for DLSw with the "dlsw local-peer peer-id <IP-address>" command listen for IP protocol 91 packets and UDP port 2067.

Cisco IOS devices listen to IP protocol 91 packets when DLSw is configured. However, it is only used if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

```
"dlsw remote-peer 0 fst <ip-address>"
```

It is possible to disable UDP processing in DLSw with the "dlsw udp-disable" command. However, disabling UDP only prevents the sending of UDP packets, it does not prevent the device from receiving and processing incoming UDP packets.

These vulnerabilities are documented in Cisco Bug ID CSCsk73104 and have been assigned Common Vulnerabilities and Exposures (CVE) ID CVE-2008-1152.

Vulnerability Scoring Details

=====

Cisco has provided scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco has provided an FAQ to answer additional questions regarding CVSS at <http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at <http://intellishield.cisco.com/security/alertmanager/cvss>

CSCsk73104 – Handling of malformed packets by DLSW

CVSS Base Score – 7.8

Access Vector: Network
Access Complexity: Low
Authentication: None

Confidentiality Impact: None
Integrity Impact: None
Availability Impact: Complete

CVSS Temporal Score – 6.4

Exploitability: Functional
Remediation Level: Official-Fix
Report Confidence: Confirmed

Impact
=====

Successful exploitation of these vulnerabilities may result in the reload of the device or memory leaks, leading to a DoS condition.

Software Versions and Fixes
=====

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) or your contracted maintenance provider for assistance.

Each row of the Cisco IOS software table (below) names a Cisco IOS release train. If a given release train is vulnerable, then the earliest possible releases that contain the fix (along with the anticipated date of availability for each, if applicable) are listed in the "First Fixed Release" column of the table. The "Recommended Release" column indicates the releases which have fixes for all the published vulnerabilities at the time of this Advisory. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. Cisco recommends upgrading to a release equal to or later than the release in the "Recommended Releases" column of the table.

Major Release	Availability of Repaired Releases	Affected 12.0-Based Releases	First Fixed Release	Recommended Release
Vulnerable;	12.0	first fixed	12.3(26)	in 12.3

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

| Releases |
| prior to |
| 12.0(8)DA3 |
| are |
| vulnerable, |
| release |
| 12.0DA | 12.0(8)DA3 |
| and later |
| are not |
| vulnerable; |
| migrate to |
| any release |
in 12.2DA

| Releases |
| prior to |
| 12.0(7)DB |
| are |
| vulnerable, |
| 12.0DB | release | 12.4(18a) |
| 12.0(7)DB |
| and later |
| are not |
| vulnerable; |
| first fixed |
in 12.4

| Releases |
| prior to |
| 12.0(7)DC |
| are |
| vulnerable, |
| 12.0DC | release | 12.4(18a) |
| 12.0(7)DC |
| and later |
| are not |
| vulnerable; |
| first fixed |
in 12.4

| Releases |
| prior to |
| 12.0(17)S5 |
| are |
| 12.0S | vulnerable, | 12.0(32)S10 |
| release |
| 12.0(17)S5 |
| and later |
| are not |
vulnerable;

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

```
|-----+-----+-----|
| 12.0SC | Not | |
| | Vulnerable | |
|-----+-----+-----|
| 12.0SL | Not | |
| | Vulnerable | |
|-----+-----+-----|
| 12.0SP | Not | |
| | Vulnerable | |
|-----+-----+-----|
| 12.0ST | Not | |
| | Vulnerable | |
|-----+-----+-----|
| 12.0SX | Not | |
| | Vulnerable | |
|-----+-----+-----|
| 12.0SY | Not | |
| | Vulnerable | |
|-----+-----+-----|
| 12.0SZ | Not | |
| | Vulnerable | |
|-----+-----+-----|
| | Vulnerable; | |
| 12.0T | first fixed | 12.3(26) |
| | in 12.3 | |
|-----+-----+-----|
| 12.0W | Vulnerable; | 12.0(3c)W5 |
| | contact TAC | (8) |
|-----+-----+-----|
| 12.0WC | Vulnerable; | |
| | contact TAC | |
|-----+-----+-----|
| 12.0WT | Not | |
| | Vulnerable | |
|-----+-----+-----|
| | Vulnerable; | |
| 12.0XA | first fixed | 12.3(26) |
| | in 12.3 | |
|-----+-----+-----|
| 12.0XB | Not | |
| | Vulnerable | |
|-----+-----+-----|
| | Releases | |
| | prior to | |
| | 12.0(2)XC2 | |
| | are | |
| | vulnerable, | |
| 12.0XC | release | 12.3(26) |
| | 12.0(2)XC2 | |
| | and later | |
| | are not | |
```

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

```
|| vulnerable; ||  
|| first fixed ||  
|| in 12.3 ||  
-----+-----+-----  
|| Vulnerable; || |
|| 12.0XD | first fixed | 12.3(26) |  
|| in 12.3 ||  
-----+-----+-----  
|| Vulnerable; || |
|| 12.0XE | first fixed ||  
|| in 12.1E ||  
-----+-----+-----  
|| 12.0XF | Not ||  
|| Vulnerable ||  
-----+-----+-----  
|| Vulnerable; || |
|| 12.0XG | first fixed | 12.3(26) |  
|| in 12.3 ||  
-----+-----+-----  
|| Vulnerable; || |
|| 12.0XH | first fixed | 12.3(26) |  
|| in 12.3 ||  
-----+-----+-----  
|| Releases || |
|| prior to ||  
|| 12.0(4)XI2 ||  
|| are ||  
|| vulnerable, ||  
|| 12.0XI | release | 12.3(26) |  
|| 12.0(4)XI2 ||  
|| and later ||  
|| are not ||  
|| vulnerable; ||  
|| first fixed ||  
|| in 12.3 ||  
-----+-----+-----  
|| Releases || |
|| prior to ||  
|| 12.0(4)XJ5 ||  
|| are ||  
|| vulnerable, ||  
|| 12.0XJ | release | 12.3(26) |  
|| 12.0(4)XJ5 ||  
|| and later ||  
|| are not ||  
|| vulnerable; ||  
|| first fixed ||  
|| in 12.3 ||  
-----+-----+-----  
|| Vulnerable; ||  
|| 12.0XK | first fixed | 12.3(26) |
```

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

```
|| in 12.3 ||  
|-----+-----+-----|  
| 12.0XL | Not ||  
| | Vulnerable ||  
|-----+-----+-----|  
| 12.0XM | Not ||  
| | Vulnerable ||  
|-----+-----+-----|  
| | Vulnerable; ||  
| 12.0XN | first fixed | 12.3(26) |  
| | in 12.3 ||  
|-----+-----+-----|  
| | Vulnerable; ||  
| 12.0XQ | first fixed | 12.3(26) |  
| | in 12.3 ||  
|-----+-----+-----|  
| | Vulnerable; ||  
| 12.0XR | first fixed | 12.3(26) |  
| | in 12.3 ||  
|-----+-----+-----|  
| 12.0XS | Not ||  
| | Vulnerable ||  
|-----+-----+-----|  
| 12.0XV | Not ||  
| | Vulnerable ||  
|-----+-----+-----|  
| 12.0XW | Not ||  
| | Vulnerable ||  
|-----+-----+-----|  
| Affected | First Fixed | Recommended |  
| 12.1–Based | Release | Release |  
| Releases |||  
|-----+-----+-----|  
| | Vulnerable; ||  
| 12.1 | first fixed | 12.3(26) |  
| | in 12.3 ||  
|-----+-----+-----|  
| | Vulnerable; ||  
| 12.1AA | first fixed | 12.3(26) |  
| | in 12.3 ||  
|-----+-----+-----|  
| 12.1AX | Not ||  
| | Vulnerable ||  
|-----+-----+-----|  
| | Releases ||  
| | prior to ||  
| | 12.1(22)AY1 ||  
| | are ||  
| 12.1AY | vulnerable, | 12.1(22) |  
| | release | EA11 |  
| | 12.1(22)AY1 ||
```

```
|| and later ||  
|| are not ||  
|| vulnerable; ||  
|-----+-----+-----|  
| 12.1AZ | Not | |  
| Vulnerable | |  
|-----+-----+-----|  
| 12.1CX | Not | |  
| Vulnerable | |  
|-----+-----+-----|  
| 12.1DA | Not | |  
| Vulnerable | |  
|-----+-----+-----|  
|| Releases || |
|| prior to ||  
|| 12.1(4)DB1 ||  
|| are ||  
|| vulnerable, ||  
|| 12.1DB | release | 12.4(18a) |  
|| 12.1(4)DB1 ||  
|| and later ||  
|| are not ||  
|| vulnerable; ||  
|| first fixed ||  
|| in 12.4 ||  
|-----+-----+-----|  
|| Releases || |
|| prior to ||  
|| 12.1(4)DC2 ||  
|| are ||  
|| vulnerable, ||  
|| 12.1DC | release | 12.4(18a) |  
|| 12.1(4)DC2 ||  
|| and later ||  
|| are not ||  
|| vulnerable; ||  
|| first fixed ||  
|| in 12.4 ||  
|-----+-----+-----|  
| 12.1E | 12.1(27b)E4 | |  
|-----+-----+-----|  
|| Releases || |
|| prior to ||  
|| 12.1(11)EA1 ||  
|| are ||  
|| 12.1EA | vulnerable, | 12.1(22) |  
|| release | EA11 |  
|| 12.1(11)EA1 ||  
|| and later ||  
|| are not ||  
|| vulnerable; ||
```

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

12.1EB	Not	Vulnerable
12.1EC	migrate to 12.3(23)BC1	any release in 12.2BC
12.1EO	Not	Vulnerable
12.1EU	Not	Vulnerable
12.1EV	Not	Vulnerable
12.1EW	Not	Vulnerable
12.1EX	first fixed	in 12.1E
12.1EY	Not	Vulnerable
12.1EZ	first fixed	in 12.1E
12.1GA	first fixed	12.3(26) in 12.3
12.1GB	first fixed	12.3(26) in 12.3
12.1T	first fixed	12.3(26) in 12.3
12.1XA	first fixed	12.3(26) in 12.3
12.1XB	Not	Vulnerable

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

```
|| Vulnerable; ||  
| 12.1XC | first fixed | 12.3(26) |  
| in 12.3 ||  
-----+-----+-----  
|| Vulnerable; ||  
| 12.1XD | first fixed | 12.3(26) |  
| in 12.3 ||  
-----+-----+-----  
| 12.1XE | Not ||  
| Vulnerable ||  
-----+-----+-----  
| 12.1XF | Not ||  
| Vulnerable ||  
-----+-----+-----  
|| Vulnerable; ||  
| 12.1XG | first fixed | 12.3(26) |  
| in 12.3 ||  
-----+-----+-----  
|| Vulnerable; ||  
| 12.1XH | first fixed | 12.3(26) |  
| in 12.3 ||  
-----+-----+-----  
|| Vulnerable; ||  
| 12.1XI | first fixed | 12.3(26) |  
| in 12.3 ||  
-----+-----+-----  
|| Vulnerable; ||  
| 12.1XJ | first fixed | 12.3(26) |  
| in 12.3 ||  
-----+-----+-----  
| 12.1XK | Not ||  
| Vulnerable ||  
-----+-----+-----  
| 12.1XL | Not ||  
| Vulnerable ||  
-----+-----+-----  
|| Vulnerable; ||  
| 12.1XM | first fixed | 12.3(26) |  
| in 12.3 ||  
-----+-----+-----  
| 12.1XN | Not ||  
| Vulnerable ||  
-----+-----+-----  
| 12.1XO | Not ||  
| Vulnerable ||  
-----+-----+-----  
|| Vulnerable; ||  
| 12.1XP | first fixed | 12.3(26) |  
| in 12.3 ||  
-----+-----+-----  
|| Vulnerable; ||
```

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

```
| 12.1XQ | first fixed | 12.3(26) |
| | in 12.3 | |
|-----+-----+-----|
| 12.1XR | Not | |
| | Vulnerable | |
|-----+-----+-----|
| | Vulnerable; | |
| 12.1XS | first fixed | 12.3(26) |
| | in 12.3 | |
|-----+-----+-----|
| | Releases | |
| | prior to | |
| | 12.1(3)XT2 | |
| | are | |
| | vulnerable, | |
| 12.1XT | release | 12.3(26) |
| | 12.1(3)XT2 | |
| | and later | |
| | are not | |
| | vulnerable; | |
| | first fixed | |
| | in 12.3 | |
|-----+-----+-----|
| 12.1XU | Not | |
| | Vulnerable | |
|-----+-----+-----|
| | Releases | |
| | prior to | |
| | 12.1(5)XV1 | |
| | are | |
| | vulnerable, | |
| 12.1XV | release | 12.3(26) |
| | 12.1(5)XV1 | |
| | and later | |
| | are not | |
| | vulnerable; | |
| | first fixed | |
| | in 12.3 | |
|-----+-----+-----|
| | Vulnerable; | |
| 12.1XW | first fixed | 12.3(26) |
| | in 12.3 | |
|-----+-----+-----|
| | Vulnerable; | |
| 12.1XX | first fixed | 12.3(26) |
| | in 12.3 | |
|-----+-----+-----|
| | Vulnerable; | |
| 12.1XY | first fixed | 12.3(26) |
| | in 12.3 | |
|-----+-----+-----|
```

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

```
|| Vulnerable; ||  
| 12.1XZ | first fixed | 12.3(26) |  
|| in 12.3 ||  
|-----+-----+-----|  
|| Vulnerable; ||  
| 12.1YA | first fixed | 12.3(26) |  
|| in 12.3 ||  
|-----+-----+-----|  
|| Vulnerable; ||  
| 12.1YB | first fixed | 12.3(26) |  
|| in 12.3 ||  
|-----+-----+-----|  
| 12.1YC | Not ||  
|| Vulnerable ||  
|-----+-----+-----|  
|| Vulnerable; ||  
| 12.1YD | first fixed | 12.3(26) |  
|| in 12.3 ||  
|-----+-----+-----|  
|| Releases ||  
|| prior to ||  
|| 12.1(5)YE1 ||  
|| are ||  
|| vulnerable, ||  
| 12.1YE | release | 12.3(26) |  
|| 12.1(5)YE1 ||  
|| and later ||  
|| are not ||  
|| vulnerable; ||  
|| first fixed ||  
|| in 12.3 ||  
|-----+-----+-----|  
| 12.1YF | Not ||  
|| Vulnerable ||  
|-----+-----+-----|  
| 12.1YG | Not ||  
|| Vulnerable ||  
|-----+-----+-----|  
| 12.1YH | Not ||  
|| Vulnerable ||  
|-----+-----+-----|  
|| Vulnerable; ||  
| 12.1YI | first fixed | 12.3(26) |  
|| in 12.3 ||  
|-----+-----+-----|  
| 12.1YJ | Not ||  
|| Vulnerable ||  
|-----+-----+-----|  
| Affected | First Fixed | Recommended |  
| 12.2-Based | Release | Release |  
| Releases |||
```

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

```
|-----+-----+-----|
| Vulnerable; |
| 12.2 | first fixed | 12.3(26) |
| in 12.3 |
|-----+-----+-----|
| Vulnerable; |
| 12.2B | first fixed | 12.4(18a) |
| in 12.4 |
|-----+-----+-----|
| 12.2BC | Not |
| Vulnerable |
|-----+-----+-----|
| Vulnerable; |
| 12.2BW | first fixed | 12.3(26) |
| in 12.3 |
|-----+-----+-----|
| Vulnerable; |
| 12.2BY | first fixed | 12.4(18a) |
| in 12.4 |
|-----+-----+-----|
| 12.2BZ | Not |
| Vulnerable |
|-----+-----+-----|
| 12.2CX | Not |
| Vulnerable |
|-----+-----+-----|
| 12.2CY | Not |
| Vulnerable |
|-----+-----+-----|
| 12.2CZ | Not |
| Vulnerable |
|-----+-----+-----|
| 12.2DA | Not |
| Vulnerable |
|-----+-----+-----|
| Vulnerable; |
| 12.2DD | first fixed | 12.4(18a) |
| in 12.4 |
|-----+-----+-----|
| Vulnerable; |
| 12.2DX | first fixed | 12.4(18a) |
| in 12.4 |
|-----+-----+-----|
| 12.2EU | Not |
| Vulnerable |
|-----+-----+-----|
| 12.2EW | Not |
| Vulnerable |
|-----+-----+-----|
| 12.2EWA | Not |
| Vulnerable |
```

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

Vulnerable; 12.2EX migrate to 12.2(40)EX1 any release in 12.2SEA
12.2EY Not Vulnerable
12.2EZ Not Vulnerable
12.2FX Not Vulnerable
12.2FY Not Vulnerable
12.2FZ Not Vulnerable
12.2IXA Vulnerable; contact TAC
12.2IXB Vulnerable; contact TAC
12.2IXC Vulnerable; contact TAC
12.2IXD Vulnerable; contact TAC
Vulnerable; 12.2(18) migrate to IXF; 12.2IXE any release Available in 12.2IXF on 31-MAR-08
12.2JA Not Vulnerable
12.2JK Not Vulnerable
12.2MB Not Vulnerable
12.2MC 12.2(15) 12.4(18a) MC2h

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

```
| 12.2S | 12.2(25)S15 | 12.2(25)S15 |
|-----+-----+-----|
|| 12.2(28) || |
|| SB10 ||
|| ||
|| 12.2(31)SB9 | 12.2(28) |
|| 12.2SB || SB12 |
|| 12.2(33)SB; ||
|| Available ||
|| on ||
|| 31-MAR-08 ||
|-----+-----+-----|
|| Vulnerable; || |
|| first fixed ||
|| in 12.2SB ||
|| ||
|| 12.2SBC | Vulnerable; | 12.2(28) |
|| first fixed | SB12 |
|| in 12.2SB; ||
|| Available ||
|| on ||
|| 31-MAR-08 ||
|-----+-----+-----|
| 12.2SCA | Not ||
| Vulnerable ||
|-----+-----+-----|
| 12.2SE | Not ||
| Vulnerable ||
|-----+-----+-----|
| 12.2SEA | Not ||
| Vulnerable ||
|-----+-----+-----|
| 12.2SEB | Not ||
| Vulnerable ||
|-----+-----+-----|
| 12.2SEC | Not ||
| Vulnerable ||
|-----+-----+-----|
| 12.2SED | Not ||
| Vulnerable ||
|-----+-----+-----|
| 12.2SEE | Not ||
| Vulnerable ||
|-----+-----+-----|
| 12.2SEF | Not ||
| Vulnerable ||
|-----+-----+-----|
| 12.2SEG | Not ||
| Vulnerable ||
|-----+-----+-----|
| 12.2SG | 12.2(44)SG | 12.2(44)SG |
```

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

```
|-----|
| 12.2SGA | Not ||
| | Vulnerable ||
|-----|
| 12.2SL | Not ||
| | Vulnerable ||
|-----|
| 12.2SM | Not ||
| | Vulnerable ||
|-----|
| 12.2SO | Not ||
| | Vulnerable ||
|-----|
| 12.2SRA | 12.2(33) | 12.2(33) |
| | SRA6 | SRA7 |
|-----|
| | 12.2(33) | 12.2(33) |
| | SRB3; | SRB3; |
| 12.2SRB | Available | Available |
| | on | on |
| | 31-MAR-08 | 31-MAR-08 |
|-----|
| 12.2SRC | Not ||
| | Vulnerable ||
|-----|
| | Vulnerable; ||
| 12.2SU | first fixed | 12.4(18a) |
| | in 12.4 ||
|-----|
| | Releases ||
| | prior to ||
| | 12.2(29a) ||
| | SV1 are ||
| | vulnerable, ||
| | release ||
| 12.2SV | 12.2(29a) | 12.2(29b)SV |
| | SV1 and ||
| | later are ||
| | not ||
| | vulnerable; ||
| | migrate to ||
| | any release ||
| | in 12.2SVA | |
|---|---|---|
| 12.2SVA | Not ||
| | Vulnerable ||
|-----|
| 12.2SVC | Not ||
| | Vulnerable ||
|-----|
| 12.2SVD | Not ||
```

```

| | Vulnerable | |
|-----+-----+-----|
| | Releases | | |
| | prior to | |
| | 12.2(25) | |
| | SW10 are | |
| | vulnerable, | |
| | 12.2SW | release | |
| | 12.2(25) | |
| | SW10 and | |
| | later are | |
| | not | |
| | vulnerable; | |
|-----+-----+-----|
| | Vulnerable; | 12.2(18) | |
| | 12.2SX | first fixed | SXF13 |
| | in 12.2SXF | |
|-----+-----+-----|
| | Vulnerable; | 12.2(18) | |
| | 12.2SXA | first fixed | SXF13 |
| | in 12.2SXF | |
|-----+-----+-----|
| | Vulnerable; | 12.2(18) | |
| | 12.2SXB | first fixed | SXF13 |
| | in 12.2SXF | |
|-----+-----+-----|
| | Vulnerable; | 12.2(18) | |
| | 12.2SXD | first fixed | SXF13 |
| | in 12.2SXF | |
|-----+-----+-----|
| | Vulnerable; | 12.2(18) | |
| | 12.2SXE | first fixed | SXF13 |
| | in 12.2SXF | |
|-----+-----+-----|
| | 12.2(18) | | |
| | SXF12 | |
| | | |
| | 12.2SXF | 12.2(18) | 12.2(18) |
| | SXF12a | SXF13 |
| | | |
| | 12.2(18) | |
| | SXF13a | |
|-----+-----+-----|
| | 12.2SXH | 12.2(33) | |
| | SXH1 | |
|-----+-----+-----|
| | Vulnerable; | 12.2(18) | |
| | 12.2SY | first fixed | SXF13 |
| | in 12.2SXF | |
|-----+-----+-----|
| | 12.2(25)S15 |

```

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

```
|| Vulnerable; ||  
| 12.2SZ | first fixed | 12.2(28) |  
|| in 12.2S | SB12 |  
|| ||  
|| | 12.2(33)SRC |  
|-----+-----+-----|  
|| Vulnerable; ||  
| 12.2T | first fixed | 12.3(26) |  
|| in 12.3 ||  
|-----+-----+-----|  
| 12.2TPC | 12.2(8) ||  
|| TPC10d ||  
|-----+-----+-----|  
| 12.2UZ | Not ||  
|| Vulnerable ||  
|-----+-----+-----|  
|| Vulnerable; ||  
| 12.2XA | first fixed | 12.3(26) |  
|| in 12.3 ||  
|-----+-----+-----|  
|| Vulnerable; ||  
| 12.2XB | first fixed | 12.3(26) |  
|| in 12.3 ||  
|-----+-----+-----|  
|| Vulnerable; ||  
| 12.2XC | first fixed | 12.4(18a) |  
|| in 12.4 ||  
|-----+-----+-----|  
|| Vulnerable; ||  
| 12.2XD | first fixed | 12.3(26) |  
|| in 12.3 ||  
|-----+-----+-----|  
| 12.2XE | Not ||  
|| Vulnerable ||  
|-----+-----+-----|  
| 12.2XF | Not ||  
|| Vulnerable ||  
|-----+-----+-----|  
|| Vulnerable; ||  
| 12.2XG | first fixed | 12.3(26) |  
|| in 12.3 ||  
|-----+-----+-----|  
|| Vulnerable; ||  
| 12.2XH | first fixed | 12.3(26) |  
|| in 12.3 ||  
|-----+-----+-----|  
| 12.2XI | Not ||  
|| Vulnerable ||  
|-----+-----+-----|  
|| Vulnerable; ||  
| 12.2XJ | first fixed | 12.3(26) |
```

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

|| in 12.3 ||
|-----+-----+-----|
	Vulnerable;	
12.2XK	first fixed	12.3(26)
	in 12.3	
-----+-----+-----		
	Vulnerable;	
12.2XL	first fixed	12.3(26)
	in 12.3	
-----+-----+-----		
	Vulnerable;	
12.2XM	first fixed	12.3(26)
	in 12.3	
-----+-----+-----		
12.2XN	12.2(33)XN1	12.3(26)
-----+-----+-----		
12.2XO	Not	
	Vulnerable	
-----+-----+-----		
	Vulnerable;	
12.2XQ	first fixed	12.3(26)
	in 12.3	
-----+-----+-----		
12.2XR	Not	
	Vulnerable	
-----+-----+-----		
12.2XS	Not	
	Vulnerable	
-----+-----+-----		
	Vulnerable;	
12.2XT	first fixed	12.3(26)
	in 12.3	
-----+-----+-----		
	Vulnerable;	
12.2XU	first fixed	12.3(26)
	in 12.3	
-----+-----+-----		
	Vulnerable;	
12.2XV	first fixed	12.3(26)
	in 12.3	
-----+-----+-----		
	Vulnerable;	
12.2XW	first fixed	12.3(26)
	in 12.3	
-----+-----+-----		
	Releases	
	prior to	
	12.2(4)YA8	
	are	
	vulnerable,	
12.2YA	release	12.3(26)

	12.2(4)YA8	
	and later	
	are not	
	vulnerable;	
	first fixed	
	in 12.3	

	Vulnerable;		
	12.2YB	first fixed	12.3(26)
	in 12.3		

	Vulnerable;		
	12.2YC	first fixed	12.3(26)
	in 12.3		

	Vulnerable;		
	12.2YD	first fixed	12.4(18a)
	in 12.4		

	12.2(25)S15		
	Vulnerable;		
	12.2YE	first fixed	12.2(28)
	in 12.2S	SB12	
	12.2(33)SRC		

	Vulnerable;		
	12.2YF	first fixed	12.3(26)
	in 12.3		

|| 12.2YG | Not ||
|| Vulnerable ||

	Vulnerable;		
	12.2YH	first fixed	12.3(26)
	in 12.3		

	Releases		
	prior to		
	12.2(8)YJ1		
	are		
	vulnerable,		
	12.2YJ	release	12.3(26)
	12.2(8)YJ1		
	and later		
	are not		
	vulnerable;		
	first fixed		
	in 12.3		

|| 12.2YK | Not ||

|| Vulnerable ||

	Vulnerable;	
12.2YL	first fixed	12.4(18a)
	in 12.4	

	Vulnerable;	
12.2YM	first fixed	12.4(18a)
	in 12.4	

	Vulnerable;	
12.2YN	first fixed	12.4(18a)
	in 12.4	

	Vulnerable;	12.2(18)
12.2YO	first fixed	SXF13
	in 12.2SXF	

| 12.2YP | Not ||
|| Vulnerable ||

| 12.2YQ | Not ||
|| Vulnerable ||

| 12.2YR | Not ||
|| Vulnerable ||

| 12.2YS | Not ||
|| Vulnerable ||

	Vulnerable;	
12.2YT	first fixed	12.3(26)
	in 12.3	

	Vulnerable;	
12.2YU	first fixed	12.4(18a)
	in 12.4	

	Releases	
	prior to	
	12.2(11)YV1	
	are	
	vulnerable,	
12.2YV	release	12.4(18a)
	12.2(11)YV1	
	and later	
	are not	
	vulnerable;	
	first fixed	
	in 12.4	

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

```
|| Vulnerable; ||  
| 12.2YW | first fixed | 12.4(18a) |  
|| in 12.4 ||  
-----+-----+-----  
|| Vulnerable; ||  
| 12.2YX | first fixed | 12.4(18a) |  
|| in 12.4 ||  
-----+-----+-----  
|| Vulnerable; ||  
| 12.2YY | first fixed | 12.4(18a) |  
|| in 12.4 ||  
-----+-----+-----  
|| | 12.2(25)S15 |  
|| Vulnerable; ||  
| 12.2YZ | first fixed | 12.2(28) |  
|| in 12.2S | SB12 |  
|| |  
|| | 12.2(33)SRC |  
-----+-----+-----  
|| Vulnerable; | 12.2(18) |  
| 12.2ZA | first fixed | SXF13 |  
|| in 12.2SXF ||  
-----+-----+-----  
|| Vulnerable; ||  
| 12.2ZB | first fixed | 12.4(18a) |  
|| in 12.4 ||  
-----+-----+-----  
| 12.2ZC | Not ||  
|| Vulnerable ||  
-----+-----+-----  
| 12.2ZD | Vulnerable; ||  
|| contact TAC ||  
-----+-----+-----  
|| Vulnerable; ||  
| 12.2ZE | first fixed | 12.3(26) |  
|| in 12.3 ||  
-----+-----+-----  
|| Vulnerable; ||  
| 12.2ZF | first fixed | 12.4(18a) |  
|| in 12.4 ||  
-----+-----+-----  
| 12.2ZG | Not ||  
|| Vulnerable ||  
-----+-----+-----  
|| Releases ||  
|| prior to ||  
|| 12.2(13)ZH6 ||  
|| are ||  
|| vulnerable, ||  
| 12.2ZH | release | 12.2(13) |  
|| 12.2(13)ZH6 | ZH11 |
```

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

```
|| and later ||
|| are not ||
|| vulnerable; ||
|| first fixed ||
|| in 12.4 || |
|---|---|---|---|
|| Vulnerable; ||
|| 12.2ZJ | first fixed | 12.4(18a) |
|| in 12.4 || |
|---|---|---|---|
|| Vulnerable; | 12.4(15)T4 |
|| 12.2ZL | first fixed ||
|| in 12.4 | 12.4(18a) | |
|---|---|---|---|
|| 12.2ZP | Not ||
|| Vulnerable || |
|---|---|---|---|
|| Vulnerable; | 12.2(33) |
|| 12.2ZU | first fixed | SXH2 |
|| in 12.2SXH || |
|---|---|---|---|
|| 12.2ZY | 12.2(18)ZY2 | 12.2(18)ZY2 |
|-----|
| Affected | First Fixed | Recommended |
| 12.3–Based | Release | Release |
| Releases ||| |
|---|---|---|---|
|| 12.3 | 12.3(24) | 12.3(26) |
|-----|
|| Vulnerable; ||
|| 12.3B | first fixed | 12.4(18a) |
|| in 12.4 || |
|---|---|---|---|
|| 12.3BC | Not ||
|| Vulnerable || |
|---|---|---|---|
|| Vulnerable; ||
|| 12.3BW | first fixed | 12.4(18a) |
|| in 12.4 || |
|---|---|---|---|
|| 12.3EU | Not ||
|| Vulnerable || |
|---|---|---|---|
|| 12.3JA | Not ||
|| Vulnerable || |
|---|---|---|---|
|| 12.3JEA | Not ||
|| Vulnerable || |
|---|---|---|---|
|| 12.3JEB | Not ||
|| Vulnerable ||
```

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

```
|-----|
| 12.3JEC | Not | |
| | Vulnerable | | |
|---|---|---|---|
| | Releases | |
| | prior to | |
| | 12.3(8)JK1 | |
| | are | |
| | 12.3JK | vulnerable, | 12.3(8)JK1 |
| | release | |
| | 12.3(8)JK1 | |
| | and later | |
| | are not | |
| | vulnerable; | |
|-----|
| 12.3JL | Not | |
| | Vulnerable | |
|-----|
| 12.3JX | Not | |
| | Vulnerable | | |
|---|---|---|---|
| | Vulnerable; | |
| | 12.3T | first fixed | 12.4(18a) |
| | in 12.4 | |
|-----|
| 12.3TPC | Not | |
| | Vulnerable | |
|-----|
| 12.3VA | Vulnerable; | |
| | contact TAC | | |
|---|---|---|---|
| | 12.3(2)XA7; | 12.3(2)XA7; |
| | 12.3XA | Available | Available |
| | on | on |
| | 31-MAR-08 | 31-MAR-08 | |
|---|---|---|---|
| | Vulnerable; | |
| | 12.3XB | first fixed | 12.4(18a) |
| | in 12.4 | | |
|---|---|---|---|
| | 12.4(15)T4 |
| | 12.3XC | 12.3(2)XC5 | |
| | 12.4(18a) | | |
|---|---|---|---|
| | Vulnerable; | |
| | 12.3XD | first fixed | 12.4(18a) |
| | in 12.4 | | |
|---|---|---|---|
| | 12.3(2)XE6; | 12.4(15)T4 |
| | 12.3XE | Available | |
| | on | 12.4(18a) |
```

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

```
|| 31-MAR-08 ||
|-----+-----+-----|
|| Vulnerable; ||
| 12.3XF | first fixed | 12.4(18a) |
|| in 12.4 ||
|-----+-----+-----|
|| Vulnerable; ||
|| first fixed | 12.4(15)T4 |
| 12.3XG | in 12.3YG; ||
|| Available | 12.4(18a) |
|| on ||
|| 16-JUN-08 ||
|-----+-----+-----|
|| Vulnerable; ||
| 12.3XH | first fixed | 12.4(18a) |
|| in 12.4 ||
|-----+-----+-----|
|| 12.3(7) ||
|| XI11; ||
| 12.3XI | Available | |
|| on ||
|| 18-SEP-08 ||
|-----+-----+-----|
|| Vulnerable; | 12.3(14) |
| 12.3XJ | first fixed | YX11 |
|| in 12.3YX ||
|| | 12.4(15)T4 |
|-----+-----+-----|
|| Vulnerable; ||
| 12.3XK | first fixed | 12.4(18a) |
|| in 12.4 ||
|-----+-----+-----|
|| Vulnerable; ||
| 12.3XQ | first fixed | 12.4(18a) |
|| in 12.4 ||
|-----+-----+-----|
|| 12.3(7)XR8; | 12.3(7)XR8; |
| 12.3XR | Available | Available |
|| on | on |
|| 31-MAR-08 | 31-MAR-08 |
|-----+-----+-----|
| 12.3XS | Not ||
|| Vulnerable ||
|-----+-----+-----|
|| Vulnerable; ||
| 12.3XU | first fixed | 12.4(15)T4 |
|| in 12.4T ||
|-----+-----+-----|
|| Vulnerable; | 12.3(14) |
| 12.3XW | first fixed | YX11 |
|| in 12.3YX ||
```

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

```
|| 12.4(15)T4 |
|-----|
| 12.3XY | Not |
| Vulnerable |
|-----|
| 12.3YA | Not |
| Vulnerable |
|-----|
| 12.3YD | Not |
| Vulnerable |
|-----|
| Vulnerable; | 12.3(14) |
| 12.3YF | first fixed | YX11 |
| in 12.3YX |
| 12.4(15)T4 |
|-----|
| 12.3(8)YG7; |
| 12.3YG | Available | 12.4(15)T4 |
| on |
| 16-JUN-08 |
|-----|
| Vulnerable; |
| 12.3YH | first fixed | 12.4(15)T4 |
| in 12.4T |
|-----|
| Vulnerable; |
| 12.3YI | first fixed | 12.4(15)T4 |
| in 12.4T |
|-----|
| Vulnerable; |
| 12.3YJ | first fixed | 12.4(15)T4 |
| in 12.4T |
|-----|
| Vulnerable; |
| 12.3YK | first fixed | 12.4(15)T4 |
| in 12.4T |
|-----|
| 12.3YM | 12.3(14) | 12.3(14) |
| YM12 | YM12 |
|-----|
| Vulnerable; |
| 12.3YQ | first fixed | 12.4(15)T4 |
| in 12.4T |
|-----|
| 12.3(11) |
| YS3; |
| 12.3YS | Available | 12.4(15)T4 |
| on |
| 31-MAR-08 |
|-----|
| Vulnerable; |
```

Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS

```
| 12.3YT | first fixed | 12.4(15)T4 |
| | in 12.4T | |
|-----+-----+-----|
| | Vulnerable; | |
| 12.3YU | first fixed | |
| | in 12.4XB | |
|-----+-----+-----|
| 12.3YX | 12.3(14) | 12.3(14) |
| | YX11 | YX11 | |
|-----+-----+-----|
| 12.3YZ | 12.3(11)YZ3 | |
|-----+-----+-----|
| Affected | First Fixed | Recommended |
| 12.4-Based | Release | Release |
| Releases | | |
|-----+-----+-----|
| | 12.4(10c) | | |
| | | |
| | 12.4(13e) | | |
| | | |
| | 12.4(16b) | | |
| 12.4 | | 12.4(18a) |
| | 12.4(17) | | |
| | | |
| | 12.4(3h) | | |
| | | |
| | 12.4(8d) | | |
|-----+-----+-----|
| 12.4JA | Not | |
| | Vulnerable | | |
|-----+-----+-----|
| 12.4JK | Not | |
|
```